

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
AT TACOMA

UNITED STATES OF AMERICA,	)	No. 3:16-cr-05110-RJB
	)	<b>ORDER ON DEFENDANTS' MOTION</b>
Plaintiff,	)	<b>TO DISMISS INDICTMENT,</b>
	)	<b>DEFENDANTS' MOTION TO</b>
v.	)	<b>SUPPRESS EVIDENCE, DEFENDANTS'</b>
	)	<b>MOTION TO EXCLUDE EVIDENCE,</b>
	)	<b>AND THIRD ORDER ON</b>
DAVID TIPPENS,	)	<b>DEFENDANTS' MOTION TO COMPEL</b>
	)	<b>DISCOVERY</b>
Defendant.	)	

UNITED STATES OF AMERICA,	)	No. 3:15-cr-00387-RJB
	)	
Plaintiff,	)	<b>ORDER ON DEFENDANTS' MOTION</b>
	)	<b>TO DISMISS INDICTMENT,</b>
v.	)	<b>DEFENDANTS' MOTION TO</b>
	)	<b>SUPPRESS EVIDENCE, DEFENDANTS'</b>
	)	<b>MOTION TO EXCLUDE EVIDENCE,</b>
	)	<b>AND THIRD ORDER ON</b>
GERALD LESAN,	)	<b>DEFENDANTS' MOTION TO COMPEL</b>
	)	<b>DISCOVERY</b>
Defendant.	)	

UNITED STATES OF AMERICA,	)	No. 3:15-cr-00274-RJB
	)	
Plaintiff,	)	<b>ORDER ON DEFENDANTS' MOTION</b>
	)	<b>TO DISMISS INDICTMENT,</b>
v.	)	<b>DEFENDANTS' MOTION TO</b>
	)	<b>SUPPRESS EVIDENCE, DEFENDANTS'</b>
	)	<b>MOTION TO EXCLUDE EVIDENCE,</b>
	)	<b>AND THIRD ORDER ON</b>
BRUCE LORENTE,	)	<b>DEFENDANTS' MOTION TO COMPEL</b>
	)	<b>DISCOVERY</b>
Defendant.	)	

THIS MATTER comes before the Court on three motions filed by Defendant David Tippens, Defendant Gerald Lesan, and Defendant Bruce Lorente (collectively, "Defendants"):

(1) Defendants’ Motion to Dismiss Indictment (Dkt. 32<sup>1</sup>), (2) Defendants’ Motion to Suppress Evidence (Dkt. 35), and (3) Defendants’ Motion to Exclude Evidence (Dkt. 31). Also before the Court are unresolved discovery matters of Defendants’ Motion to Compel. *See* Dkts. 54, 73, 78, 80, 81, 90. The Court has considered the parties’ responsive briefings and supplements thereto (Dkts. 54, 56, 58, 61, 62, 64, 74, 75, 77, 86, 92, 96, 98, 100, 101, 104, 105), evidence and oral argument presented at public hearings held on October 31, 2016 and November 1, 2016 and at an *in camera* hearing held on October 31, 2016 (*see transcript*, Dkts. 102, 103), pleadings filed pursuant to Classified Information Procedures Act (CIPA) 18 U.S.C. App. 3 §§2 and 4 (Dkts. 86, 92, 95), and the remainder of the file herein.<sup>2</sup>

## I. BACKGROUND

### A. Website A

On February 19, 2015, with the authorization of a warrant issued pursuant to 18 U.S.C. § 2510 *et seq.*, the FBI took control of Website A, a website “dedicated” to child pornography, and relocated the site to a government server in Newington, Virginia. The site had more than 100,000 registered member accounts and 1,500 daily visitors. Dkt. 37-1 at ¶¶6, 11, 19. According to an FBI affiant, the homepage, which required users to login to proceed, featured “prepubescent females partially clothed and whose legs are spread with instructions for joining the site before one can enter.” *Id.* ¶10. The homepage was changed to feature one youthful female before the warrant was issued, but after the affidavit was prepared.

---

<sup>1</sup> Docket numbers refer to *United States v. Tippens*, 3:16-cr-05110-RJB, except where otherwise noted. Defendant Lesan and Defendant Lorente filed identical motions, and this order equally pertains to all three cases.

<sup>2</sup> This Court is also assigned *United States v. Michaud*, No. 3:15-5351-RJB (W.D.Wash. 2016), a companion case arising from the same FBI investigation. The presentation in these cases overlap with the showing in *Michaud*, but different and additional presentations have been made here.

1 After logging in, registered users would view a page with hyperlinks to forum topics,  
2 the clear majority of which advertised child pornography. Dkt. 37-1. at ¶¶14-18. Website A  
3 operated on the Tor network, a publicly available alternative internet service that allows users  
4 to mask identifying information, such as Internet Protocol (“IP”) addresses. *Id.* at ¶¶9, 10.

5 **B. The Network Investigating Technique (NIT)**

6 With Website A under its control, on February 20, 2015, the FBI submitted a warrant  
7 application to authorize use of a Network Investigating Technology (NIT). Dkt. 37-1. To  
8 explain how the NIT works, the Government has offered the declaration and testimony of Dr.  
9 Brian Levine. Dkts. 58-1, 102. Defendants have incorporated the declaration of four experts,  
10 Vlad Tsyklevich, Matthew Miller, Robert Young, and Shawn Kasal. Dkts. 31-2, 31-3, 31-4,  
11 31-5. Mr. Tsyklevich explained how the NIT works as follows:

13 The NIT presented by the FBI works by using an “exploit,” a piece of software that  
14 takes advantage of a software “vulnerability” in the Tor Browser program. By  
15 exploiting this software vulnerability, the NIT is able to circumvent the security  
16 protections in the Tor Browser, which under normal circumstances, prevents web sites  
17 from determining the true IP address or MAC address of visitors. After exploiting the  
18 vulnerability, the NIT delivers a software “payload,” a predetermined set of actions, to  
19 computers that receive the payload (the “host computer”). The payload used by the FBI  
20 in this case collected and then transmitted identifying information about the host  
21 computer (including its IP address) along with a unique “identifier” used to associate  
22 the target with the identifying information that the NIT collects.

23 Dkt. 31-2 at ¶4. According to Mr. Tsyklevich, the NIT has four primary components:

- 24 a. Software that generates a payload and injects a unique identifier into it.
- 25 b. The “exploit” that is sent to the target computer to take advantage of a software flaw  
26 in the Tor Browser.
- 27 c. The “payload” that is run on the target computer to extract identifying information  
28 about it (such as its IP address).
- 29 d. An additional “server component” that stores and preserves the extracted information  
30 and allows investigators to access it.

1 *Id.*

2 **C. The NIT warrant**

3 The FBI submitted the February 20, 2015 warrant application in the Eastern District of  
 4 Virginia to Magistrate Judge Theresa Buchanan. According to the warrant application, the NIT  
 5 causes “activating computers” to “transmit certain information to a computer controlled by or  
 6 known by the government . . . that may assist in identifying the user’s computer, its location,  
 7 and the user of the computer.” Dkt. 37-1 at 33.

8 The face sheet to the NIT Warrant expressly incorporates two attachments and reads as  
 9 follows:  
 10

11 An application by a federal law enforcement officer . . . requests the search of the  
 12 following person or property located in the Eastern District of Virginia  
*(identify the person or describe the property to be searched and give its location):*

13 See Attachment A

14 The person or property to be searched, described above, is believed to conceal *(identify*  
 15 *the person or describe the property to be seized):* See Attachment B[.]

16 Dkt. 37-2 at 1.

17 Attachment A reads as follows:

18 Attachment A

19 Place to be Searched

20 This warrant authorizes the use of a network investigative technique (“NIT”) to  
 21 be deployed on the computer server described below, obtaining information described  
 22 in Attachment B from the activating computers below.

23 The computer server is the server operating the Tor network child pornography  
 24 website referred to herein as the TARGET WEBSITE, as identified by its URL –  
 [omitted]— which will be located at a government facility in the Eastern District of  
 25 Virginia.

26 The activating computers are those of any user or administrator who logs into  
 the TARGET WEBSITE by entering a username and password. The government will

1 not employ this network investigative technique after 30 days after this warrant is  
2 authorized, without further authorization.

3 Dkt. 37-2 at 2.

4 Attachment B reads as follows:

5 Attachment B

6 Information to be Seized

7 From any “activating” computer described in Attachment A:

- 8 1. the “activating” computer’s actual IP address, and the date and time that the  
9 NIT determines what that IP address is;  
10 2. a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or  
11 special characters) to distinguish data from that other “activating” computers, that  
12 will be sent with and collected by the NIT;  
13 3. the type of operating system running on the computer, including type (e.g.,  
14 Windows), version (e.g., Windows 7), and architecture (e.g., x 86);  
15 4. information about whether the NIT has already been delivered to the “activating”  
16 computer;  
17 5. the “activating” computer’s Host Name;  
18 6. the “activating” computer’s active operating system username; and  
19 7. the “activating” computer’s media access control (“MAC”) address;

20 Dkt. 37-2 at 3.

21 **D. Deployment of the NIT**

22 For approximately 14 days, from February 20, 2015 through March 4, 2015, the FBI  
23 administered Website A from a government-controlled computer server located in Virginia,  
24 which forwarded a copy of all website communications to FBI personnel in Linthicum,  
25 Maryland. Once deployed by the Government, the NIT gathered approximately nine thousand  
26 IP addresses, approximately seven thousand of which were associated with computers in one of  
more than one-hundred countries other than United States. Dkt. 90-1 at 3, 5. The FBI maintains  
that it did not post content itself, but concedes that it allowed registered users to access the site,  
view and download child pornographic content for distribution, and post new content,

1 including 44 “new” series of data. *Id.* at 3. Some website users commented on technical  
2 improvements to the site while under FBI control. Dkt. 90-3. A NIT has been relied on by the  
3 FBI in at least twenty-three other investigations. Dkt. 100.

#### 4 **E. Local warrants**

5 Based on IP addresses and other identifying information gathered by use of the NIT,  
6 officers used databases and other law enforcement tools to develop probable cause to search  
7 Defendants’ home residences and vehicles. *See generally*, Dkt. 37-3.<sup>3</sup> Warrants were issued by  
8 a magistrate judge in the Western District of Washington to search addresses within this  
9 district. *Id.* Execution of the local warrants resulted in the seizure of computers and other  
10 media devices found to contain child pornography, and allegedly belonging to Defendants.

#### 12 **F. Procedural history and motions**

13 All three defendants are charged in Count I with receipt of child pornography, and in  
14 Count II with possession of child pornography. *United States v. Tippens*, 3:16-cr-05110-RJB at  
15 Dkt. 15; *United States v. Lesan*, 3:15-cr-000387-RJB at Dkt. 13; *United States v. Lorente*,  
16 3:15-cr-00274-RJB at Dkt. 11. *See* 18 U.S.C. § 2252 (a)(2), (b)(1) (receipt) and (a)(4), (b)(2)  
17 (possession).

18 In Defendants’ Motion to Dismiss, Defendants argue that dismissal is warranted based  
19 on outrageous government conduct. Dkt. 32.

20 Defendants’ Motion to Suppress challenges the NIT Warrant on two primary grounds:  
21 (1) lack of probable cause, and (2) violations of the United States Magistrate Judges Act, 28  
22 U.S.C. § 636, and Fed. R. Crim. P. 41(b). Dkt. 35.

---

23  
24  
25  
26 <sup>3</sup> The affidavit cited to is particular only to Defendant Tippens, *see* Dkt. 37-3, but Defendants have consolidated their arguments and make no effort to distinguish one affidavit from another.

1 In Defendants' Motion to Exclude, Defendants argue that if they are denied the  
2 opportunity to review the NIT code in its entirety, the Court should exclude all evidence  
3 derived from the NIT code, including evidence found on the computers seized by law  
4 enforcement. Dkt. 31. The Government has provided to Defendants "one component of the  
5 payload." Dkt. 31-2 at ¶5. At oral argument held on October 31, 2016 and November 1, 2016,  
6 the parties agreed that the Government has more recently provided some portions of other  
7 components, although the parties have differing views on the significance of the material  
8 provided. Dkt. 102 at 11, 12.

9  
10 To bolster its formal objection to turning over the entire NIT code, the Government  
11 requested the opportunity to conduct a CIPA §4 *ex parte*, *in camera* hearing. Dkt. 86 at 2. The  
12 Government also requested the opportunity to explain at that hearing why it should not be  
13 required to produce discovery responsive to two discovery requests, Request #5 and Request  
14 #8, which were the subject of two prior discovery orders. *Id.* See Dkts. 54, 80, 81. The Court  
15 granted the request for the CIPA § 4 hearing. Dkt. 95. On October 31, 2016, following the  
16 Government's *ex parte* and *in camera* presentation, the Court found that, based on the showing  
17 made, the Government was not required to disclose the remaining NIT code or discovery  
18 responsive to Request #5 or Request #8. Dkt. 102 at 116.

19  
20 The Court also granted the Government's request to conduct a CIPA § 2 pretrial  
21 hearing. Dkt. 95 at 2. *See* Dkt. 86 at 2. At hearings held on October 31, 2016 and November 1,  
22 2016, Defendants offered no evidence to supplement the written record.

23 The Government offered to stipulate for trial purposes that an exploit can make changes  
24 to security settings that would allow a third party to run commands on a computer without the  
25 computer user's knowledge. Dkt. 103 at 65, 66. No stipulation was reached. *Id.* at 71.

## II. DISCUSSION

### A. Motion to Dismiss (based on outrageous conduct)

It is easy to conclude that the Government acted outrageously here:

(1) The Government ignored the statute forbidding such conduct: “In any criminal proceeding, any property or material that constitutes child pornography . . . shall remain in the care, custody and control of either the Government or the Court.” 18 U.S.C § 3509(m).

(2) The Government facilitated the continued availability of Website A, a site containing hundreds of child pornographic images for criminal users around the world.

(3) The Government, in fact, improved Website A’s technical functionality.

(4) The Government re-victimized hundreds of children by keeping Website A online.

(5) The Government used the child victims as bait to apprehend viewers of child pornography without informing the victims and without the victims’ permission—or that of their families.

(6) The Government’s actions placed any lawyer involved in jeopardy for violating ABA Model Rules of Professional Conduct 8.4, and raise serious ethical and moral issues for counsel. *See also*, Washington Rules of Professional Conduct 8.4.

The only justification for the acts of the Government, as provided by counsel, is that the end justifies the means, or in the Government’s words, “Because those who create, obtain, trade, distribute and profit from the imagery of the rape and sexual exploitation of children have turned to Tor in an effort to hide their activities, the United States has been forced to



1 employ creative means to unmask the individuals engaging in the destructive and heinous  
2 criminal conduct.” Dkt. 101 at 3.

3 Nevertheless, dismissal of criminal charges due to outrageous conduct by the  
4 Government requires consideration of much more than the requisite conduct. “Dismissing an  
5 indictment for outrageous conduct . . . is limited to extreme cases in which the defendant can  
6 demonstrate that the government’s conduct violates fundamental fairness,” which is “an  
7 extremely high standard.” *United States v. Black*, 733 F.3d 294, 302 (9<sup>th</sup> Cir. 2013) (internal  
8 quotations and citations omitted). Under *Black*, “there is no bright line” test to determine  
9 whether law enforcement’s conduct is outrageous, but the following factors should be  
10 considered: (1) known criminal characteristics of the defendants; (2) individualized suspicion  
11 of the defendants; (3) the government’s role in creating the crime of the conviction; (4) the  
12 government’s encouragement to commit the offensive conduct; (5) the nature of the  
13 government’s participation in the offense conduct; and (6) the balance between the nature of  
14 the crime and the necessity of the conduct. *Id.* at 303.

16 *Black* has provided examples of the types of cases where dismissal is warranted:

17  
18 It is outrageous for government agents to engineer and direct a criminal enterprise from  
19 start to finish . . . to use excessive physical or mental coercion to convince an individual  
20 to commit a crime [and] . . . to generate new crimes merely for the sake of pressing  
21 criminal charges.

22 *Id.* (internal quotations and citations omitted). Conversely, under *Black*, it is not outrageous  
23 conduct “to infiltrate a criminal organization, to approach individuals who are already involved  
24 in or contemplating a criminal act . . . to provide necessary items to a conspiracy. . . [or] to  
25 use artifice and stratagem to ferret out criminal activity.” *Id.* at 303 (internal quotations and  
26 citations omitted).

1 Applying the *Black* factors: (1) the Government did not know the criminal  
2 characteristics of any defendant; (2) the Government had no individualized suspicion of any  
3 defendant; (3) the Government created an opportunity for others to commit the crimes charged,  
4 but did not create the crimes charged; (4) the Government did not encourage the crimes  
5 charged—only provided the opportunity to persons unknown; (5) the nature of the  
6 Government’s participation was only to provide an opportunity to commit the crimes charged;  
7 and (6) reasonable minds can differ over the balance between the nature—and potential  
8 number—of the crimes charged and the necessity for the Governmental conduct, as reflected in  
9 the Government’s justification for its conduct.  
10

11 Considering the totality of the circumstances, Defendants have not shown that dismissal  
12 based on outrageous government conduct is warranted. Defendants’ motion to dismiss should  
13 be denied.

#### 14 **B. Motion to Suppress**

15 Defendants’ motion to suppress challenges the NIT Warrant in two primary ways: (1)  
16 lack of probable cause, and (2) violations of the United States Magistrate Judges Act, 28  
17 U.S.C. § 636, and Fed. R. Crim. P. 41(b).

##### 18 *1. Probable cause*

19 The Fourth Amendment prohibits “unreasonable searches and seizures” and requires  
20 that “no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and  
21 particularly describing the place to be searched and the persons or things to be seized.”  
22 U.S.Const. Amend. IV. Whether a warrant is supported by probable cause is a totality of the  
23 circumstances test that relies on common sense, where the magistrate judge weighs whether  
24 there is a “fair probability” that contraband or evidence will be found in a particular place.  
25  
26

1 *United States v. Gourde*, 440 F.3d 1065, 1069 (9<sup>th</sup> Cir. 2006), citing *Illinois v. Gates*, 462 U.S.  
2 213, 214 (1983).

3 Defendants argue that the NIT Warrant lacks probable cause because it did not describe  
4 with particularity how Website A “unabashedly announce[d]” that it was an illegal child  
5 pornography site, and that the NIT Warrant amounts to an invalid anticipatory warrant. Dkt. 35  
6 at 27-32. Neither argument is persuasive. First, the FBI affiant provided sufficient detail for a  
7 reasonable magistrate judge to conclude that Website A was an illegal child pornography site.  
8 The FBI affiant described in detail the homepage, which featured two prepubescent, partially-  
9 clothed females, as well as text instructing users how to post photos and video material. Dkt.  
10 37-1 at ¶¶12, 13. The website was not publicly available and could be found only by using a  
11 Tor hidden service. *Id.* at ¶¶6-9. The FBI affiant described the items to be gathered by use of  
12 the NIT, which, for a period of 30 days, was authorized to be deployed only against registered  
13 users of the child pornography site. *Id.* at ¶34. When weighing the totality of the circumstances,  
14 the NIT Warrant does not fail for lack of probable cause, especially because the magistrate  
15 judge was permitted to rely on the conclusions of the FBI affiant about “where evidence is  
16 likely to be found.” *United States v. Terry*, 911 F.2d 272, 274 (9<sup>th</sup> Cir. 1990). *See* Dkt. 37-1 at  
17 ¶¶6-37. The fact that the homepage was changed from two prepubescent females to one  
18 youthful female between the time that the FBI affidavit was prepared and when the NIT  
19 Warrant was issued is immaterial to this conclusion.

22 Second, although the NIT Warrant may be an anticipatory warrant, as in *United States*  
23 *v. Gourde*, 440 F.3d 1065, 1071 (9<sup>th</sup> Cir. 2006), the NIT Warrant in this case did not seek to  
24 inculcate the “unwitting[], or even passive[]” site visitor. The NIT Warrant was not triggered  
25 until a person had logged onto a website with a homepage that prominently displayed an  
26

underage, under-clothed female. Unlike the website in *Gourde*, which could be found with a Google search of a word, “Lolita,” *id.*, Website A could not be found by use of a Google search and instead required knowledge of the exact address, which was extremely unlikely to be stumbled on. Dkt. 37-1 at ¶10. The NIT Warrant does not fail for lack of probable cause.

2. 28 U.S.C. § 636

Defendants argue that the NIT Warrant is void because it violated 28 U.S.C. § 636, a violation distinct from the Rule 41(b) violation (discussed below). Dkt. 35 at 2. The United States Magistrates Act, codified at 28 U.S.C. §§ 631-639, provides:

(a) Each United States magistrate judge . . . shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law—

(1) all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts[.]

28 U.S.C. § 636(a) (emphasis added).

Section 636 and Rule 41(b) have nearly identical language, and § 636 incorporates Rule 41(b), *see* § 636(a)(1), so it is not clear that § 636 violations should be analyzed separately from Rule 41(b) violations. *Compare* § 636 (“ . . . magistrate judge[s] shall have within the district . . . all powers and duties conferred . . . by the Rules of Criminal Procedure”); *and* Fed. R. Crim. P. 41(b)(1) (“a magistrate judge with authority in the district . . . has authority to issue a warrant to search for . . . property located within the district”). Other courts have unified the analysis, which may be a better way to reconcile the two rules. *See, e.g., United States v. Broy*, 2016 WL 5172853, at \*6 (C.D. Ill. Sept. 21, 2016). Nonetheless, analyzing the NIT Warrant through the lens of § 636, it was lawful for the magistrate judge to authorize deployment of the NIT to search computers within her district, which may have been her intent, but deployment of the NIT resulted in the search of Defendants’ computers in the Western District of

1 Washington and elsewhere, which exceeded the boundaries of the magistrate judge's  
2 jurisdiction.

3 To the extent that the NIT Warrant authorized the search of computers outside of the  
4 Eastern District of Virginia, the NIT Warrant violated § 636.

5 3. *Fed. R. Crim. P. 41(b)*

6 Fed. R. Crim. P. 41(b)(1), which has the force of a statute, *see* 18 U.S.C. § 3103, sets  
7 out the general rule that “a magistrate with authority in the district . . . has the authority to issue  
8 a warrant to search for and seize a person or property located within the district.” The rule also  
9 carves out exceptions, two of which apply, according to the Government: (1) subdivision  
10 (b)(2), where a person or property “might move or be moved outside the district before the  
11 warrant is executed,” and (2) subdivision (b)(4), which authorizes “install[ing] within the  
12 district a tracking device . . . to track the movement of a person located within the district,  
13 outside the district, or both[.]” Rule 41(b) is to be applied flexibly, not rigidly, especially as to  
14 technology. *United States v. Koyomejian*, 970 F.2d 536, 542 (9<sup>th</sup> Cir. 1992). In *United States v.*  
15 *New York Tel. Co.*, 434 U.S. 159 (1977), the court noted that a flexible reading of the rule is  
16 reinforced by Fed. R. Crim. P. 57(b), which provides that in the absence of controlling law, “a  
17 judge may regulate practice in any manner consistent with federal law, these rules and the local  
18 rules[.]” *Id.*, at 170.

19 Rule 41 subdivisions (b)(2) and (b)(4) did not authorize the search of computers in the  
20 Western District of Washington or elsewhere beyond the magistrate judge's district. To so  
21 interpret those rules appears to stretch their plain language far beyond their intent. Even when  
22 flexibly applying the rule, the NIT Warrant violated the letter of Rule 41(b).  
23  
24  
25  
26

1 Having determined that the NIT Warrant violates Rule 41(b), the next issue is whether  
2 the violation was fundamental or technical. “Fundamental errors are those that result in clear  
3 constitutional violations,” which warrant suppression. *United States v. Negrete-Gonzales*, 966  
4 F.2d 1277, 1283 (9th Cir. 1992) (internal citations omitted). Technical errors warrant  
5 suppression only if: (1) there is evidence of deliberate disregard of the rule, or (2) the  
6 defendants were prejudiced by the error “in the sense that the search would not have occurred .  
7 . . if the rule had been followed or would have been less intrusive absent the error.” *Id.*

8 Defendants argue that a fundamental violation of constitutional magnitude occurred due  
9 to the “unprecedented worldwide warrant . . . the cyber equivalent of the general warrants that  
10 were anathema to the Founders.” Dkt. 74 at 15. The Court previously rejected the lack of  
11 particularity argument, finding probable cause for issuance of the NIT Warrant. *See § IIB1*  
12 *above*. Defendants have not shown that the Rule 41(b) violation was fundamental.

14 Because the Rule 41(b) violation was not fundamental, it was technical, and  
15 suppression is warranted only if there is a requisite showing of deliberate disregard of Rule  
16 41(b) or prejudice. *See United States v. Negrete-Gonzales*, 966 F.2d 1277, 1283 (9th Cir.  
17 1992). Defendants’ argument that the Government acted with deliberate disregard of Rule  
18 41(b) is unavailing. As evidence of deliberate disregard, Defendants point to a Department of  
19 Justice letter to the Chair of the Advisory Committee on the Criminal Rules, Dkt. 37-8 at 1,  
20 which was sent on September 18, 2013, a date prior to when the FBI sought the NIT Warrant  
21 in this case. The DOJ letter proposed changes to Rule 41(b) to “better enable law enforcement  
22 to investigate and prosecute botnets and crimes involving Internet anonymizing technologies,”  
23 because “Rule 41(b) does not directly address the special circumstances that arise . . . where  
24 the warrant sufficiently describes the computer to be searched but the district . . . is unknown.”  
25  
26

1 *Id.* (emphasis added). Defendants’ argument would require the Court to make inferences not  
2 required by the text of the DOJ letter. The DOJ letter reveals an intent to improve the rule,  
3 which does not rule out the possibility that DOJ could have considered Rule 41(b) sufficiently  
4 flexible to address changes in technology. *See also*, Dkt. 104-1. Furthermore, the record is  
5 silent as to the magistrate judge’s thoughts regarding the scope of the warrant at the time it was  
6 issued, and speculation on that subject is fruitless. The record does not show deliberate  
7 disregard.

8  
9 Defendants also argue that Defendants were prejudiced, because “if the rule had been  
10 heeded . . . [and] the NIT searches . . . properly confined to the Eastern District of Virginia,”  
11 there would have been no search of Defendants’ computers. *Id.* at 10, 11. The definition of  
12 prejudice relied upon by Defendants, “in the sense that the search would not have occurred if  
13 the rule had been followed,” found in *United States v. Weiland*, 420 F.3d 1062, 1071 (9<sup>th</sup> Cir.  
14 2005), should not be construed broadly. Under Defendants’ interpretation, all searches  
15 executed on the basis of warrants in violation of Rule 41(b) would result in prejudice, no  
16 matter how small or technical the error might be. Tracing the *Weiland* definition to its prior  
17 application within the Ninth Circuit, *see United States v. Vasser*, 648 F.2d 507, 511 (9<sup>th</sup> Cir.  
18 1980), a more workable interpretation of the *Weiland* definition inquires whether evidence  
19 obtained from a warrant that violates Rule 41(b) could have been available by other lawful  
20 means, and if so, the defendant did not suffer prejudice.

22 Applied here, Defendants did not suffer prejudice when they revealed to a third party  
23 the key identifying information, their IP addresses, to which they had no reasonable  
24 expectation of privacy. *United States v. Forrester*, 512 F.3d 500, 510 (9<sup>th</sup> Cir. 2008). As  
25 another court within this circuit explained:  
26

1 The FBI was ultimately able to locate [the defendant] by tracking his IP address to his  
2 internet provider, demonstrating that [the defendant] voluntarily turned his IP address  
3 information over to this third party so that it could provide him with web services . . .  
As [the defendant] does not have an expectation of privacy in his IP address, the FBI  
could have legally discovered [the defendant's] IP address absent the NIT Warrant.

4 *United States v. Henderson*, 15-CR-00565-WHO-1 at 7 (N.D.Cal. Sept. 9, 2016). The fact that  
5 Defendants may have attempted to hide their IP addresses does not change the analysis,  
6 because the focus is on the reasonableness of, not Defendants' subjective efforts to protect, the  
7 expectation of privacy.

8 The Rule 41(b) violation was technical, not fundamental, and suppression is not  
9 warranted based on the violation.

10  
11 *4. Good faith exception*

12 Given the violations of Rule 41(b) and § 636, the next issue is whether the good faith  
13 exception bars application of the exclusionary rule. Determining whether to apply the good  
14 faith exception to the exclusionary rule where the warrant is issued by a detached and neutral  
15 magistrate judge "must be resolved by weighing the costs and benefits of preventing the use . .  
16 . of inherently trustworthy tangible evidence . . . that ultimately is found to be defective."  
17 *United States v. Leon*, 468 U.S. 897, 906–07 (1984) (internal citations and quotations omitted).  
18 Whether a warrant is executed in good faith depends on whether reliance on the warrant was  
19 objectively reasonable. If reliance was objectively reasonable, the good faith exception applies,  
20 because "excluding the evidence will not further the ends of the exclusionary rule" to deter  
21 police misconduct. *Id.* at 918. The determination of whether the good faith exception applies  
22 "is an issue separate" from whether constitutional rights were violated by police conduct. *Id.* at  
23 918 (citations and quotations omitted). The exclusionary rule does not apply to deter  
24 misconduct of judges or magistrates, because "there exists no evidence suggesting that . . .  
25  
26



1 lawlessness among [judges and magistrates] actors requires application of the extreme sanction  
2 of exclusion.” *Id.* at 916.

3 In this case, reliance on the NIT Warrant was objectively reasonable. The NIT Warrant,  
4 issued by a magistrate judge, authorized deploying the NIT from a government-controlled  
5 computer server in the Eastern District of Virginia for up to 30 days to search “activating  
6 computers.” Dkt. 37-2. The NIT Warrant defined “activating computers” as computers of “any  
7 user or administrator who logs into [Website A],” from which the FBI was authorized to gather  
8 IP addresses and other identifying information. Dkt. 37-2 at 3. The FBI affiant detailed the  
9 need for the NIT, based on the nature of Website A, a child pornography site hidden on the Tor  
10 network. Dkt. 37-1 at ¶¶9-37. The FBI affiant also described the mechanics of deploying the  
11 NIT and the scope of the items to be searched and seized. *Id.* The NIT Warrant authorized  
12 solely what was requested by the FBI affiant. Dkt. 37-1 at ¶34; Dkt. 37-2 at 2, 3. Based on  
13 these facts, relying on the NIT Warrant was objectively reasonable. The record does not  
14 support a finding that the magistrate judge was misled, that the magistrate judge wholly  
15 abandoned her role as detached and neutral decisionmaker, that the warrant was issued based  
16 on a total lack of probable cause, or other grounds to reject the good faith exception. *See Leon*,  
17 468 U.S. at 923-24.  
18  
19

20 Defendants argue that the good faith exception should not excuse the Rule 41(b)  
21 violation. Dkt. 74 at 24, 25. Under *United States v. Negrete-Gonzales*, 966 F.2d 1277, 1283  
22 (9th Cir. 1992), “[f]undamental errors are those that result in clear constitutional violations . . .  
23 [and] require suppression, unless the officers can show good faith reliance as required by  
24 *Leon*.” *Id.* “To take advantage of *Leon*, the executing agents . . . must demonstrate an  
25 objectively reasonable basis for their mistaken belief that the warrant was valid.” *Id.* (emphasis  
26

1 omitted). For technical errors, suppression is required “only if: (1) the defendants were  
2 prejudiced by the error, or (2) there is evidence of deliberate disregard of the rule.” *Id.* In this  
3 case the Rule 41(b) violation was technical, and as previously discussed, there has not been a  
4 showing of prejudice or deliberate disregard. Even if the Rule 41(b) violation was fundamental,  
5 because reliance was objectively reasonable, the Rule 41(b) violation need not warrant  
6 suppression.

7 Defendants also argue that the good faith exception does not excuse the § 636 violation,  
8 Dkt. 74 at 25, but this Court is not aware of any authority that would require exclusion of  
9 evidence where officers acted in good faith. Some courts have argued that the *Leon* good faith  
10 exception should not extend to the NIT Warrant because the warrant was void *ab initio*. *See*,  
11 *e.g.*, *United States v. Levin*, 2016 WL 2596010, at \*10 (D. Mass. May 5, 2016). *Leon* does not  
12 make the void *ab initio* distinction urged by Defendants and the court in *Levin*. *Levin* conceded  
13 that this is an unresolved area of the law. *Id.* The NIT Warrant was not void *ab initio*, because  
14 it was valid at least as to computers within the issuing magistrate judge’s district, but even if it  
15 was void *ab initio*, § 636 restricts only magistrate judges. The exclusionary rule does not apply  
16 to deter the conduct of magistrate judges, who are “neutral judicial officers [who] have no  
17 stake in the outcome of particular criminal prosecutions. *Leon*, 468 U.S. at 916-17. *See also*,  
18 *United States v. Negrete-Gonzales*, 966 F.2d 1277, 1283 (9th Cir. 1992); *Illinois v. Krull*, 480  
19 U.S. 340, 348 (1987).

22 The NIT Warrant violated Rule 41(b) and § 636, but because reliance on the warrant  
23 was objectively reasonable, the good faith exception bars application of the exclusionary rule.  
24 Defendants’ motion to suppress should be denied.

25 **C. Motion to Exclude Evidence**  
26

1 Based on the Motion to Exclude (Dkt. 31) and the Motion to Compel Discovery (Dkt.  
2 54), Defendants seek remaining discovery:

3 (1) Opportunity to review the NIT code in its entirety;

4 (2) Request #5: “The names of all agents, contractors, or other personnel who assisted  
5 with relocating, maintaining and operating Playpen while it was under Government  
6 control”; and

7 (3) Request #8: “Copies of all correspondence, referrals, and other records indicating  
8 whether the exploit . . . has been submitted by the FBI . . . to the White House’s  
9 Vulnerability Equities Process (VEP) and what, if any, decision was made by the  
10 VEP.”

11 Defendants ask the Court for dismissal if the requested discovery is not provided.

12 While the Government has provided certain information about the NIT to Defendants, it  
13 has objected to producing the NIT code in its entirety. The Government requested a CIPA § 4  
14 hearing, which was conducted *ex parte* and *in camera* on the subject of the NIT and the two  
15 discovery requests. (The latter were the subjects of prior orders. *See* Dkts. 80, 81.) Following  
16 the CIPA § 4 hearing, the Court ruled that it would not compel the Government to produce any  
17 of the subject discovery. Also following the CIPA § 4 hearing, the Government suggested a  
18 substitute summary of evidence. Defense counsel appeared disinterested in that approach, and  
19 no agreement was reached and no order made. 103 at 65, 66, 71. A substitute summary is,  
20 however, still available to the parties.

21 The Court also granted the Government’s request to conduct a CIPA § 2 pretrial  
22 hearing. Dkt. 95 at 2. *See* Dkt. 86 at 2. CIPA § 2 allows defendants and their attorneys to make  
23 admissions not later admissible at trial, 18 U.S.C. App. 3 § 2, but Defendants offered no  
24 evidence to supplement the written record.

25 This state of affairs leads to two issues: (1) whether the withheld material is  
26 discoverable under Fed. R. Crim. P. 16, and (2) whether the withheld material is relevant and

1 helpful to the defense. As discussed below, different standards apply to each issue. If the  
2 material is not discoverable, that ends the inquiry. If the discovery is material but not relevant  
3 and helpful, that too ends the inquiry. If the evidence is both material and relevant and helpful,  
4 the government will have to produce the material or face dismissal.

5 “Congress passed CIPA to prevent the problem of ‘graymail,’ where defendants  
6 pressed for the release of classified information to force the government to drop the  
7 prosecution.” *United States v. Sarkissian*, 841 F.2d 959, 965 (9<sup>th</sup> Cir. 1988). CIPA permits “the  
8 trial judge to rule on questions of admissibility involving classified information before  
9 introduction of the evidence in open court. . . [which] permits the government to ascertain the  
10 potential damage to national security of proceeding with a given prosecution.” *Id.* (internal  
11 citations omitted). CIPA should not be interpreted to “expand or restrict established principles  
12 of discovery . . . [or to] have a substantive impact on the admissibility of probative evidence.”  
13 *United States v. Sedaghaty*, 728 F.3d 885, 903 (9<sup>th</sup> Cir. 2013) (internal citations omitted).  
14 Instead, CIPA “clarif[ies] the court’s powers . . . to deny or restrict discovery in order to  
15 protect national security.” *Id.* at 904.

16 CIPA § 2 gives parties the option to move for a pretrial conference “to consider matters  
17 relating to classified information that may arise in connection with the prosecution.” 18 U.S.C.  
18 App. 3 § 2. At this hearing, “the court may consider any matters which relate to classified  
19 information or which may promote a fair and expeditious trial,” and to that end, “[n]o  
20 admission made by the defendant or by any attorney for the defendant . . . may be used against  
21 the defendant unless . . . in writing and [] signed[.]” *Id.*

22 CIPA § 4 provides that the Government may request an *ex parte* hearing to make a  
23 showing that, if sufficient, “may authorize the United States to delete specified items of  
24  
25  
26

1 classified information from documents to be made available to the defendant through discovery  
 2 under the Federal Rules of Criminal Procedure[.]” 18 U.S.C. App. 3 § 4. That section also  
 3 authorizes the Government “to substitute a summary of the information for such classified  
 4 documents, or to substitute a statement admitting relevant facts that the classified information  
 5 would tend to prove.” *Id.*

6 *Sedaghaty* sets out the three-step analysis for CIPA § 4 motions. First, “a district court  
 7 must first determine whether, pursuant to the Federal Rules of Criminal Procedure, statute, or  
 8 the common law, the information at issue is discoverable at all.” *United States v. Sedaghaty*,  
 9 728 F.3d 885, 904 (9<sup>th</sup> Cir. 2013). Second, the court must “determine whether the government  
 10 has made a formal claim of the state secrets privilege, lodged by the head of the department  
 11 which has actual control over the matter, after actual personal consideration by that officer.” *Id.*  
 12 Third, the court must consider whether the evidence is “relevant and helpful to the defense of  
 13 an accused,” *id.*, quoting *Roviaro v. United States*, 353 U.S. 53, 60-61 (1957), and if so,  
 14 “CIPA § 4 empowers the court to determine the terms of discovery, if any.” *Id.* (emphasis  
 15 added).  
 16

#### 17 *I. Discoverable?*

18 Under Fed. R. Crim. P. 16(a)(1)(E), the Government is required to produce discovery  
 19 that is “within the government’s possession, custody, or control and . . . is material to preparing  
 20 the defense.” The term “defense” refers to discovery that would “refute the Government’s  
 21 arguments that the defendant committed the crime charged . . . [including] discovery related to  
 22 the constitutionality of a search or a seizure.” *United States v. Soto Zuniga*, \_\_F.3d\_\_ 2016 WL  
 23 4932319 (9<sup>th</sup> Cir. 2016). The NIT code and other requested discovery is discoverable under  
 24  
 25  
 26

1 Fed. R. Crim. P. 16(a)(1)(E) because of its potential bearing on Defendants' motions, including  
2 the constitutional challenges to the NIT Warrant.

3 2. *State secrets privilege?*

4 Based on the Government's filing (Dkt. 86), which invoked a formal claim of privilege,  
5 the Court issued a sealed order, the Order Setting [Section 2] Pretrial Conference, Appointing  
6 [Classified Information Security Officer], and Granting Leave to File Section 4 Pleading. Dkt.  
7 95. Following the *ex parte* and *in camera* hearing and filings, the Court previously  
8 concluded—and now reaffirms its conclusion—that the Government made a sufficient showing  
9 to justify withholding the remaining portions of the NIT code and other discovery from  
10 Defendants.  
11

12 3. *Relevant and helpful?*

13 There is limited Ninth Circuit case law to guide courts in conducting the *Roviaro*  
14 relevant and helpful inquiry, but another District Court in the Ninth Circuit has analyzed the  
15 issue at length. *See United States v. Turi*, 143 F.Supp.3d 916, 920 (D.Ariz. 2015). This Court  
16 joins the *Turi* court in interpreting “relevant and helpful” to mean that the Government must  
17 disclose information—or face dismissal—“only if there is a reasonable probability that, had the  
18 evidence been disclosed to the defense, the result . . . would have been different.” *Id.* at 921,  
19 quoting *Klimavicius-Viloria*, 144 F.3d 1249, 1261 (9<sup>th</sup> Cir. 1998). *See also, Kyles v. Whitley*,  
20 514 U.S. 419, 436-37 (1995) (right to fair trial not violated “every time the government . . .  
21 chooses not to disclose evidence that might prove helpful”). As *Turi* explained, this standard  
22 “ensure[s] that a defendant will not be denied a fair trial for national security reasons, while  
23 requiring disclosure of classified information only when truly necessary—when the classified  
24 information would affect the result of the proceeding.” *Id.* To interpret the standard otherwise  
25  
26

1 would, for all practical purposes, conflate the discoverable inquiry with the relevant and  
 2 helpful inquiry, depriving the Court of any meaningful discretion to balance the Government's  
 3 interest in protecting classified national security information with Defendants' interest in  
 4 accessing pretrial discovery.

5 The Court is reluctant to make a "relevant and helpful" finding under CIPA § 4. To do  
 6 so, the Court must attempt to place itself in the shoes of defense counsel and examine the  
 7 evidence *ex parte* and *in camera* to determine the effect of the evidence on the defense case, if  
 8 any. Substituting a judge's mind for the fertile minds of defense counsel presents obvious risks  
 9 to due process and a fair trial. Nevertheless, in rare cases such as this one, it must be done.  
 10

11 At oral argument, Defendants referred to their experts' declarations, which Defendants  
 12 contend articulate why the Government must produce the entire NIT code. Dkt. 102 at 11; Dkt.  
 13 103 at 7, 8, 14-16. The Court now turns to three rationales offered in the declaration of Mr.  
 14 Tyrklevich, whose declaration is the most detailed of Defendants' four expert declarations, *see*  
 15 Dkts. 31-2, 31-3, 31-4, 31-5, and a fourth rationale emphasized at oral argument, *see* Dkt. 31-3  
 16 at ¶2, to determine whether the full NIT code, and other requested discovery, is relevant and  
 17 helpful to Defendants.  
 18

19 *(1) The software that generates a payload and injects a unique identifier into it*  
 20 *(component "a") is critical to understanding whether the unique identifier used to*  
 21 *link a defendant to access of illegal content is actually unique. If the identifier is*  
 22 *generated incorrectly, it could cause different users to be incorrectly linked to each*  
 23 *other's actions . . . Without the missing data, I am unable to make a determination*  
 24 *about these issues. Dkt. 31-2 at ¶6 (emphasis added).*

25 Assuming that "different users [were] incorrectly linked to each other other's actions,"  
 26 that would result in the transmission to the FBI of incorrect payload information. Then the  
 unique identifier would not necessarily correspond to the correct IP address or other identifying  
 information. The local search warrants relied on the identifying information, so if incorrect,

1 this would at worst would result in the search of the wrong home, which would not affect  
 2 Defendants here. *See United States v. Turner*, 770 F.2d 1508 (9<sup>th</sup> Cir. 1985) (warrant is  
 3 sufficiently particular absent a showing of any reasonable probability that another premise  
 4 might be mistakenly searched); *United States v. Mann*, 389 F.3d 869, 876 (9<sup>th</sup> Cir. 2004) (“the  
 5 practical accuracy [of the search warrant] rather than the technical precision governs”).  
 6 Officers relied on the identifying information in good faith. *C.f. United States v. Collins*, 830  
 7 F.2d 145 (9<sup>th</sup> Cir. 1987) (search of wrong address due to carelessness and lack of common  
 8 prudence). Furthermore, the search of Defendants’ homes was premised not on absolute  
 9 certainty, but rather on a finding of probable cause, which is a “commonsense, practical  
 10 question,” *United States v. Kelley*, 482 F.3d 1047, 1050 (9<sup>th</sup> Cir. 2007), and the theoretical  
 11 possibility of an incorrect unique identifier, which would result in the pursuit of an  
 12 investigation at the wrong address would not undermine the linchpin of probable cause.  
 13

14 (2) . . . *Analyzing and understanding the exploit component of the NIT is critical to*  
 15 *understanding whether the payload data that has been provided in discovery was*  
 16 *the only component executing and reporting information to the government or*  
 17 *whether the exploit executed additional functions outside of the scope of the NIT*  
 18 *warrant. Without the missing data about the exploit component of the NIT, I am*  
 19 *unable to make a determination about these issues.* Dkt. 31-2 at ¶6 (emphasis  
 20 added).

21 This rationale theorizes that the NIT, as deployed, may have exceeded the scope of the  
 22 NIT Warrant as authorized, but Defendants offer nothing to support this theory beyond  
 23 speculation. A careful review of the affidavits underlying the local warrants shows reliance on  
 24 the NIT only for identifying information, such as IP addresses, that fall within the scope of the  
 25 NIT Warrant. *See* Dkt. 37-3 at 79-82, ¶¶28-42. Even if the NIT “executed additional functions”  
 26 not authorized by the warrant, the remedy would be to suppress unlawfully-gained evidence,  
 not to suppress lawfully-obtained evidence that formed the basis for the local warrants. *See*  
*United States v. Payton*, 573 F.3d 859, 864 (9<sup>th</sup> Cir. 2009).



1 (3) *In addition, the server component that stores the identifying information returned*  
 2 *by the payload (component “d”) must faithfully store and reproduce the data it was*  
 3 *sent. . . [A]nalyzing this component of the NIT [is] essential to understanding and*  
 4 *verifying the digital “chain of custody” of information derived from the NIT. . . [or]*  
 5 *I am unable to make a determination about these issues. Dkt. 31-2 at ¶6 (emphasis*  
 6 *added).*

7 This rationale fails even under the assumption that there was an interruption to the  
 8 “digital chain of custody” between Defendants’ computers and the FBI server that stored the  
 9 information gathered from deployment of the NIT. If there was an interruption, by a hacker, for  
 10 example, it would at worst corrupt the “identifying information returned by the payload” used  
 11 to execute local warrants. That would not be fatal to the warrants, especially where officers  
 12 relied on the identifying information in good faith. *See subsection (1) above.*

13 The digital chain of custody argument theoretically has more bearing on the charge  
 14 against Defendants for receipt of child pornography, depending on how the Government elects  
 15 to show the “knowing receipt” of child pornography. The Government denies the need to rely  
 16 on any NIT information at trial, but Defendants are justifiably wary of this representation. As  
 17 to both counts, however, Defendants’ argument suffers from the same problem, namely, that  
 18 Defendants have provided only speculation, not facts, to support their argument.

19 (4) *Vulnerability to a third party attack that “planted” child pornography on*  
 20 *Defendants’ computers and compromised computer security settings. Dkt. 31-3 at*  
 21 *¶2.*

22 Defendants argue that analyzing the remainder of the NIT code, and the exploit in  
 23 particular, is necessary to determine whether a third party could have accessed Defendants’  
 24 computers to “plant” the child pornography. Declarations by Defendants’ experts contend that  
 25 this is a real possibility. Dkt. 31-3 at ¶2. However, when pushed by the Government to make a  
 26 stronger showing beyond arguing that such a third party attack is theoretically possible,

1 Defendants argued that they are in a “Catch-22” dilemma, because they cannot make a further  
2 showing without review of the NIT code that they seek.

3 Defendants’ “apparent Catch-22 is more apparent than real.” *United States v. Yunis*,  
4 867 F.2d 617, 624 (D.C. Cir. 1989). Defendants have concededly not conducted forensic  
5 investigations of computers seized by law enforcement, and according to the Government,  
6 conducting an investigation of the computers, along with the portions of the NIT code already  
7 disclosed, would be sufficient to determine third party vulnerability. Defendants insist that they  
8 should not need to rely on the Government’s representation, but again, Defendants have  
9 submitted no factual evidence beyond the theoretical.  
10

11 For all four rationales raised, but perhaps especially so for the fourth rationale,  
12 Defendants’ lack of showing is particularly problematic when Defendants had a unique chance  
13 for a free bite of the proverbial apple. Under CIPA § 2, Defendants have the chance to make  
14 admissions to the Court not admissible against them at trial. *See* 18 U.S.C. App. 3 § 2 (“No  
15 admission made by the defendant or by any attorney for the defendant . . . may be used against  
16 the defendant unless . . . is in writing and is signed by the defendant and [his] attorney”); FRE  
17 801(d)(2). Defendants did not avail themselves of the opportunity. Such a showing may have  
18 moved their argument beyond the theoretical, but the Court is otherwise left with Defendants’  
19 mere speculation.  
20

21 The CIPA § 4 *ex parte* and *in camera* hearing did not reveal any information to  
22 persuade the Court that production of the entire NIT would change the probability of a  
23 different outcome beyond Defendants’ speculation.

24 The Court finds that disclosing the NIT code in its entirety would not be relevant and  
25 helpful to the defense. Although Defendants provide persuasive arguments in the abstract,  
26

1 upon close examination, and in light of the record provided, Defendants have not shown the  
2 reasonable probability of a different outcome if the NIT is produced in its entirety. The  
3 remaining NIT code, though discoverable as material under Fed. R. Crim. P. 16(a)(1)(E), is not  
4 relevant and helpful to the defense under *Roviaro* and *Sedaghaty* and need not be disclosed to  
5 Defendants.

6 **D. Third Order on Defendants' Motion to Compel Discovery**

7 The Court previously found the information requested by Request #5 to be discoverable  
8 and the Government's privilege showing to be sufficient (Dkts. 80, 81), so the sole issue as to  
9 Request #5 is whether the requested discovery is relevant and helpful. *See United States v.*  
10 *Turi*, 143 F.Supp.3d 916, 920 (D.Ariz. 2015); *Roviaro v. United States*, 353 U.S. 53, 60-61  
11 (1957). The Government's *ex parte* and *in camera* presentation revealed to the Court nothing  
12 that would change the probability of a different outcome of dispositive motions or trial. The  
13 Court finds that the requested information pertaining to Request #5 is not relevant and helpful  
14 to the defense, and its production should not be compelled.

15  
16 Production of the subject matter of Request #8 should likewise not be compelled. Even  
17 if the Court assumes that the requested information is discoverable and that the Government's  
18 privilege showing is sufficient, the requested information pertaining to Request #8 is not  
19 relevant and helpful to the defense. Production of the requested information should not be  
20 compelled.

21  
22 Not only do Defendants base their request for the NIT information, Request #5, and  
23 Request #8 on speculation, but also the Court's examination of the evidence—from the file  
24 contents, from public hearings, and from *ex parte* and *in camera* hearings—leads to the  
25 conclusion that there is no evidence or information in what the Government may withhold that  
26

1 would be relevant or helpful to Defendants, that is, there is not a reasonable probability of a  
2 different outcome if the material were disclosed to Defendants.

3 \* \* \*

#### 4 **IV. CONCLUSION**

5 The new technology used to investigate Defendants presents unique  
6 constitutional and statutory challenges. As the Court previously noted in *Michaud*,  
7 “[t]he Fourth Amendment incorporates a great many specific protections against  
8 unreasonable searches and seizures. The contours of these protections in the context of  
9 computer searches pose difficult questions.” *United States v. Adjani*, 452 F.3d 1140,  
10 1152 (9th Cir. 2006)(internal quotations and citations omitted). The Government’s  
11 conduct cannot be condoned, but the charges were not dismissible as outrageous. The  
12 Government did not violate search and seizure standards enshrined in the United States  
13 Constitution. The NIT Warrant violated Rule 41(b) and § 636, but reliance on the  
14 warrant was objectively reasonable, and Defendants’ speculation about what the  
15 remaining NIT code could show does not change the outcome here.  
16

17 \* \* \*

18  
19 THEREFORE, it is HEREBY ORDERED:

20 (1) As to *United States v. Tippens*, 3:16-cr-05110-RJB:

- 21       ▪ Defendants’ Motion to Dismiss Indictment (Dkt. 32) is DENIED.
- 22       ▪ Defendants’ Motion to Suppress Evidence (Dkt. 35) is DENIED.
- 23       ▪ Defendants’ Motion to Exclude Evidence (Dkt. 31) is DENIED.
- 24       ▪ Production of the information requested in Defendants’ Motion to Compel  
25       Discovery in Request #5 and Request #8 (Dkt. 54) shall not be compelled.  
26

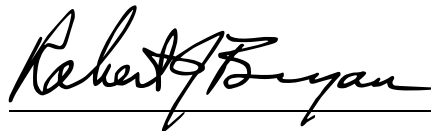
1 (2) As to *United States v. Lesan*, 3:16-cr-00387-RJB:

- 2       ▪ Defendants' Motion to Dismiss Indictment (Dkt. 82 ) is DENIED.
- 3       ▪ Defendants' Motion to Suppress Evidence (Dkt. 85) is DENIED.
- 4       ▪ Defendants' Motion to Exclude Evidence (Dkt.81) is DENIED.
- 5       ▪ Production of the information requested in Defendants' Motion to Compel
- 6       Discovery in Request #5 and Request #8 (Dkt. 100) shall not be compelled.

7 (3) As to *United States v. Lorente*, 3:15-cr-00274-RJB:

- 8       ▪ Defendants' Motion to Dismiss Indictment (Dkt. 95) is DENIED.
- 9       ▪ Defendants' Motion to Suppress Evidence (Dkt.98) is DENIED.
- 10       ▪ Defendants' Motion to Exclude Evidence (Dkt.94) is DENIED.
- 11       ▪ Production of the information requested in Defendants' Motion to Compel
- 12       Discovery in Request #5 and Request #8 (Dkt. 113) shall not be compelled.

13 DONE this 30<sup>th</sup> day of November, 2016.

14 

15 ROBERT J. BRYAN

16 United States District Judge

17

18

19

20

21

22

23

24

25

26